MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2022/2023

TAC3121 – APPLIED CRYPTOGRAPHY

(All sections / Groups)

7 JULY 2023
9.00 a.m. – 11.00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 4 pages including the cover page with **FIVE** questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1

Question 1 contains **5 MCQ questions**, please select the best answer and write your answer in the Answer Booklet provided.

(a) Which of the following is **NOT** a permutation cipher? [2 marks]

A. Rail Fence cipher
B. Block Transposition cipher
C. Product cipher
D. Geometric Figure

(b) Which of the following is **NOT** true about El Gamal encryption? [2 marks]

A. It is not secure against chosen plaintext attack.
B. It is not secure against chosen ciphertext attack.
C. Its security is based on the intractability of Discrete Logarithm problem.
D. None of the above

(c) Which of the following statements is **NOT** true regarding message authentication code (MAC) and hash function? [2 marks]

A. A hash function produces authentication if a secret key is applied.
B. Both MAC and hash function are one-way function.
C. CMAC and HMAC are examples of MAC.
D. Both MAC and hash function can be used to create digital signature.

(d) Which of the following statements is **NOT** true about Digital Signature Algorithm (DSA)? [2 marks]

A. The security of DSA is based on the difficulty of Discrete Logarithm problem.
B. The signature $s = (a, 0)$ is not a safe signature.
C. DSA always produces the same signature on the same message for different executions.
D. A secure hash function SHA-1 is used in the signature generation.

(e) Which of the following statements is **NOT** true about public key certification? [2 marks]

A. It binds the user's identity and a public-private key pair.
B. It is created by a trusted third party called certification authority.
C. The key information can be shared with other users by transmitting its certificate.
D. Anyone can verify the signature on the certificate using the signer's public key.

Continued...

Question 2

(a) State Fermat's Theorem, and use it to compute $5^{100} \bmod 7$. [4 marks]

(b) Decrypt the following ciphertext using Caesar cipher with key $K = 5$:
XNRUQJ YJXY [3 marks]

(c) Alice and Bob wish to exchange a session key using the Diffie-Hellman key exchange protocol. They have agreed to use prime modulus $q = 13$ and generator $\alpha = 3$. Alice chooses a secret number $a = 5$ and Bob chooses a secret number $b = 7$. What is the value of the session key that they establish? [3 marks]

Question 3

Given that Bob has the following RSA parameters:

RSA Parameters
$p = 3, q = 11, e = 7$

(a) Show that $e = 7$ is a valid public exponent. [3 marks]

(b) Using the given parameters, compute Bob's private key d. [3 marks]

(c) Alice intends to send a message $m = 9$ to Bob. What is the ciphertext? [2 marks]

(d) Bob receives another ciphertext $C = 19$. What is the plaintext? [2 marks]

Continued...

Question 4

(a) State the outputs of the DES S-box S_2 given the inputs 110000 and 111001 respectively.

S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

[4 marks]

(b) Double-DES is vulnerable to the meet-in-the-middle attack. Briefly describe this attack. [3 marks]

(c) If a bit error occurs in the transmission of a ciphertext character in a DES 16-bit cipher feedback (CFB) mode, how many plaintext characters are affected? State the reason. [3 marks]

Question 5

(a) Compare the security between public key cryptographic schemes and private key cryptographic schemes. Justify your answer. [3 marks]

(b) Why must any public key encryption algorithm resist chosen plaintext attack (CPA)? [3 marks]

(c) Explain what is meant by an existential forgery, an adversarial goal against a digital signature scheme. [2 marks]

(d) Both digital signature and message authentication code (MAC) provide data integrity. A digital signature also provides non-repudiation but not a MAC. Why not? [2 marks]

End of Page